## Standard Development Timeline

*This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.*

### Development Steps Completed

1. The SC authorized moving the SAR forward ~~to~~for standard development at their June 9, 2011 meeting.
2. The SAR was posted for informal comment June 10 – July 11, 2011.
3. Draft 1 of PRC-004-3 was posted for a 30-day formal comment period from June 10 – July 11, 2011.
4. Draft 2 of PRC-004-3 was posted for a 45-day ~~concurrent~~formal comment ~~and initial ballot~~ period from July 25 – September 7, 2012~~.~~ and an initial ballot in the last ten days of the comment period from August 29 – September 7, 2012.
5. Draft 3 of PRC-004-3 was posted for a 30-day formal comment period from January 22 – February 20, 2013 and a successive ballot in the last ten days of the comment period from February 11-20, 2013.

### Description of Current Draft

The Protection System Misoperations Standard Drafting Team (PSMSDT) is posting Draft ~~3~~4 of PRC-004-3 ~~posted – Protection System Misoperation Identification and Correction~~ for a ~~30~~45-day ~~formal~~ comment period ~~with parallel successive~~and ballot~~.~~ in the last ten days of the comment period under the new Standards Process Manual (Effective: June 26, 2013).

| Anticipated Actions | Anticipated Date |
|---|---|
| ~~30~~Additional 45-day Formal Comment Period with ~~Successive~~Parallel Ballot | January~~,~~ 201~~3~~4 |
| ~~Recirculation ballot~~10-day Final Ballot | ~~February, 2013~~March 2014 |
| BOT Approval | May~~,~~ 201~~3~~4 |

### Effective Dates~~: First day of~~

Except in the ~~first calendar quarter that is twelve months beyond the date that this~~ Western Interconnection, the standard ~~is approved by applicable regulatory authorities, or in those jurisdictions where regulatory approval is not required, the standard becomes~~and definitions shall become effective on the first day of the first calendar quarter that is twelve months ~~beyond the date this standard is approved by~~ after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. Except in the Western Interconnection, where approval by an applicable governmental authority is not

required, the standard and definitions shall become effective on the first day of the first calendar quarter that is twelve months after the date the standard is adopted by the NERC Board of Trustees~~,~~ or as otherwise ~~made effective pursuant to the laws applicable~~ provided for in that jurisdiction.

In the Western Interconnection, the standard and definitions shall become effective on the first day of the first calendar quarter that is twenty-four months after the date that the standard is approved by an applicable governmental authority or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to ~~such ERO governmental authorities~~go into effect. In the Western Interconnection, where approval by an applicable governmental authority is not required, the standard and definitions shall become effective on the first day of the first calendar quarter that is twenty-four months after the date the standard is adopted by the NERC Board of Trustees or as otherwise provided for in that jurisdiction.

## Version History

| Version | Date | Action | Change Tracking |
|---|---|---|---|
| 1 | TBD | Project 2010-05.1 – Protection Systems: Phase 1 (Misoperations) | New |
| | | | |
| | | | |

## Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the *Glossary of Terms used in NERC Reliability Standards* ~~*Glossary of Terms*~~ are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the ~~*G*~~glossary.

**Composite Protection System:**

The total complement of the Protection System(s) that function collectively to protect an Element, such as any primary, secondary, local backup, and communication-assisted relay systems. Backup protection provided by a remote Protection System is excluded.

**Misoperation:**

The failure of ~~an Element's composite~~a Composite Protection System to operate as intended. Any of the following is ~~*considered*~~ a Misoperation:

1. **Failure to Trip ~~–~~ During Fault ~~–~~** A failure of a Composite Protection System to operate for a Fault ~~within the zone~~ condition for which it is designed ~~to protect~~. The failure of a Protection System component is not a Misoperation as long as the ~~overall~~ performance of the Composite Protection System ~~for the Element it is designed to protect~~ is correct.

2. **Failure to Trip ~~–~~ Other Than Fault ~~–~~** A failure of a Composite Protection System to operate for a non-Fault condition for which ~~the Protection System was intended to operate~~it is designed, such as a power swing, ~~under-voltage, over-excitation~~undervoltage, overexcitation, or loss of excitation. The failure of a Protection System component is not a Misoperation as long as the ~~overall~~ performance of the Composite Protection System ~~for the Element it is designed to protect~~ is correct.

3. **Slow Trip ~~–~~ During Fault ~~–~~** A Composite Protection System operation that is slower than ~~intended~~required for a Fault ~~within the zone~~ condition for which it is designed ~~to protect~~. Delayed ~~Fault~~ clearing ~~associated with an installed high-speed protection scheme is not~~ of a Fault condition is a Misoperation if ~~the~~ high-speed performance ~~has not been~~was previously identified ~~to meet the~~ as being necessary to prevent voltage or dynamic ~~stability performance requirements of the TPL standards nor is it required to ensure coordination with~~instability, or resulted in the operation of any other Composite Protection System~~s~~.

4. **Slow Trip ~~–~~ Other Than Fault ~~–~~** A Composite Protection System operation that is slower than ~~intended~~required for a non-Fault condition for which it is designed, such as a power swing, ~~under-voltage, over-excitation~~undervoltage, overexcitation, or loss of excitation ~~for which the Protection System was intended to operate~~. Delayed clearing of a non-Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or resulted in the operation of any other Composite Protection System.

5. **Unnecessary Trip ~~–~~ During Fault** ~~– A –~~ An unnecessary Protection System operation for a Fault ~~for which the Protection System is not intended to operate.~~ condition on another Element.

6. **Unnecessary Trip ~~–~~ Other Than Fault** ~~– A –~~ An unnecessary Protection System operation for a non-Fault condition for which ~~the~~it is not designed. A Protection System ~~is not intended to operate, and~~operation that is ~~unrelated to~~caused by on-site maintenance, testing, inspection, construction, or commissioning activities is not a Misoperation.

*When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.*

## A. Introduction

1. **Title:** **Protection System Misoperation Identification and Correction**
2. **Number:** PRC-004-3
3. **Purpose:** Identify and correct the causes of Misoperations of Protection Systems for Bulk Electric System (BES) ~~Protection Systems~~Elements.
4. **Applicability:**
   - **4.1. Functional Entities:**
     - **4.1.1** Transmission Owner
     - **4.1.2** Generator Owner
     - **4.1.3** Distribution Provider
   - **4.2. Facilities:**
     - ~~**4.2.1**~~ Protection Systems for BES Elements
     - ~~**4.2.2 Underfrequency Load Shedding (UFLS) that trips a BES Element**~~
     - ~~**4.2.3 Special Protection Systems (SPS), Remedial Action Schemes (RAS), and Undervoltage Load Shedding (UVLS) are excluded**~~
     - ~~4.2.4~~4.2.1 . Non-protective functions that ~~may be imbedded~~are embedded within a Protection System are excluded. Protective functions intended to operate as a control function during switching are excluded.[1]
     - **4.2.2** Underfrequency load shedding (UFLS) that is intended to trip one or more BES Elements.

**Rationale for Applicability:** Protection Systems that protect BES Elements are integral to the operation and reliability of the BES. Some functions of relays are not used as protection but as control functions or for automation; therefore, any operation of the control function portion or the automation portion of relays is excluded from this standard. See the Application Guidelines for detailed examples of non-protective functions. Special Protection Systems (SPS) and Remedial Action Schemes (RAS) are not included in this standard because they are planned to be handled in the second phase of this project.

5. **Background**:

   A key element for BES reliability is the correct performance of Protection Systems. ~~Monitoring BES~~The monitoring of Protection System events for BES Elements, as well

[1] For additional information and examples, see the "Non-Protective Functions" and "Control Functions" sections in the Application Guidelines.

as identifying and correcting the causes of Misoperations, will improve Protection System performance. This Reliability Standard PRC-004-3 – Protection System Misoperation Identification and Correction is a revision of PRC-004-~~2a~~2.1a – Analysis and Mitigation of Transmission and Generation Protection System Misoperations ~~with the stated purpose: Ensure all transmission and generation Protection System Misoperations affecting the reliability of the Bulk Electric System (BES) are analyzed and mitigated. .~~ The Reliability Standard PRC-003-1 – Regional Procedure for Analysis of Misoperations of Transmission and Generation Protection Systems ~~required the Regions~~requires Regional Entities to establish procedures for analysis of Misoperations. In FERC Order No. 693, the Commission identified PRC-003-0 as a "fill-in-the-blank" standard. The Order stated that because the regional procedures had not been submitted, the Commission proposed not to approve or remand PRC-003-0. Because PRC-003-0 (now PRC-003-1) is not enforceable, there is not a mandatory requirement for Regional Entity procedures to support the requirements of PRC-004-~~2a.~~ 2.1a. This is a potential reliability gap; consequently, PRC-004-3 combines the reliability intent of the two legacy standards PRC-003-1 and PRC-004-~~2a~~2.1a.

This project includes revising the existing definition of Misoperation, which reads:

**Misoperation**

- Any failure of a Protection System element to operate within the specified time when a fault or abnormal condition occurs within a zone of protection.
- Any operation for a fault not within a zone of protection (other than operation as backup protection for a fault in an adjacent zone that is not cleared within a specified time for the protection for that zone).
- Any unintentional Protection System operation when no fault or other abnormal condition has occurred unrelated to on-site maintenance and testing activity.

In general, this definition needs more specificity and clarity. The terms "specified time" and "abnormal condition" are ambiguous. In the third bullet, more clarification is needed as to whether an unintentional Protection System operation for an atypical yet explainable condition is a Misoperation.

The SAR for this project also includes clarifying reporting requirements. Misoperation data, as currently collected and reported, is not ~~usable~~optimal to establish consistent metrics for measuring Protection System performance. As such, the ~~drafting team is removing the~~ data reporting obligation ~~from the~~for this standard is being removed and is ~~developing a data request~~being developed under ~~Section 1600 of~~ the NERC Rules of Procedure~~.~~, Section 1600 – Request for Data or Information ("data request"). As a result of the data request, NERC will analyze the data to: develop meaningful metrics; identify trends in Protection System performance that negatively impact reliability; identify remediation techniques; and publicize lessons learned for the industry. ~~The data submitted as part of the data request will not be used for compliance or enforcement purposes. The~~ The removal of the data collection obligation from the standard does not result in a reduction of reliability ~~as Responsible Entities are required to retain~~. The standard and data request have been developed in a manner such that evidence ~~of~~used for

compliance ~~for audit and compliance purposes under the Compliance Section C 1.2 Evidence Retention portion of~~with the standard and data request are intended to independent of each other.

The proposed requirements of the revised Reliability Standard PRC-004-3 meet the following objectives:

- ~~•~~ Review all Protection System operations on the BES to identify those that are Misoperations of Protection Systems for Facilities that are part of the BES.
- ~~•~~ Analyze Misoperations of Protection Systems for Facilities that are part of the BES to ~~determine~~identify the cause(s).
- ~~•~~ Develop and implement Corrective Action Plans to address the cause(s) of Misoperations of Protection Systems for Facilities that are part of the BES.

Misoperations ~~of or~~ associated with Special Protection Schemes~~,~~ (SPS) and Remedial Action Schemes~~, and Under-Voltage Load Shedding~~ (RAS) are not addressed in this standard due to their inherent complexities. NERC ~~intends~~plans to ~~address these areas through future projects~~handle SPS and RAS in the second phase of this project.

~~Note that the WECC~~The Western Electric Coordinating Council (WECC) Regional Reliability Standard PRC-004-WECC-1 – Protection System and Remedial Action Scheme Misoperation relates to the reporting of Misoperations of Protection Systems and RAS for a limited set of WECC Paths ~~and Remedial Action Schemes. In those cases where PRC-004~~. The WECC ~~-1 overlaps with the Continent-wide~~ region plans to conduct work to harmonize the regional standard~~, entities are expected to comply with the more stringent~~ with this continent-wide proposed standard and the second phase of this project concerning SPS and RAS.

**6. Effective Dates:** See Implementation Plan

## B. Requirements and Measures

**R1.** Each Transmission Owner, Generator Owner, and Distribution Provider ~~shall~~that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation when: *[Violation Risk Factor: Medium][Time Horizon: Operations Assessment, Operations Planning]*

~~**1.1** Within 120 calendar days of a BES interrupting device operation in its Facility caused by a Protection System operation, identify and review each Protection System operation.~~

- ~~If the entity owns both the BES interrupting device and the Protection System, determine if it was a correct operation or a Misoperation.~~
- ~~If the entity owns the~~**1.1** The BES interrupting device ~~but does not own all of the Protection System and cannot determine that the Protection System operation was correct, then notify the other owner(s) of the Protection System component(s) and provide any requested investigative information.~~

~~**Rationale for R1**: This requirement is the first step to ensuring that practices for reviewing and classifying Protection System operations and correcting Misoperations are consistently employed. The drafting team believes 120 calendar days takes into account the seasonal nature of Protection System operations; both the volume of Protection System operations as well as outage constraints for investigative purposes can be seasonal. This requirement mandates entities identify and review Protection System operations. Risks to the BES caused by Misoperations are reduced by reviewing all Protection System operations and investigating any Misoperations to find their cause(s). Requirement R1 places the responsibility on the BES interrupting device owner to investigate operations initiated by a Protection System. The initial investigation documentation should be provided to the owner of the Protection System component(s) that contributed to the Misoperation, upon request. The owner of the interrupting device and the entity that owned the component that contributed to the Misoperation should be communicating about the operation before this notification is transmitted. The owner of the component that contributed to the Misoperation will create the CAP, action plan or declaration required by Requirements R2 and R3.~~

- ~~The Protection System component owner(s) that was notified by the BES interrupting device owner shall determine if there was a correct operation or a Misoperation of their component.~~

~~Within the same 120 day period of a BES interrupting device operation~~ operation was caused by a Protection System ~~operation, the owner of the Protection System component identified as contributing to the Misoperation shall investigate and document the findings for each Misoperation including a cause, if identified.~~or by manual intervention in response to a Protection System failure to operate; and

~~**M1.** Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence for Part 1.1 that may include, but is not limited to, dated lists, logs, or a database (electronic or hard copy format) that documents the date and time of each applicable interrupting device operation and indicates when each related Protection System operation was reviewed. Acceptable evidence for the notification required by Part 1.1 may include, but is not limited to, emails, electronic files, or hard copy records demonstrating transmittal of information. Acceptable evidence for Part 1.2 may include, but is not limited to, dated lists, logs, or a database (electronic or hard copy format) that documents the date, time, Facility and equipment name associated with each Misoperation, a copy of a dated Misoperation investigation report or documented findings, which may include sequence of events, relay targets, summary of DME records for each Misoperation.~~

**1.2** The BES interrupting device owner owns all or part of the Composite Protection System; and

**1.3** The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation.

**M1.** Acceptable evidence for Requirement R1, including Parts 1.1, 1.2, and 1.3 may include, but is not limited to, the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

**Rationale for R1:** This requirement ensures that entities review those Protection System operations meeting the criteria in all three Parts (1.1, 1.2, and 1.3) and identify any that are Misoperations. The BES interrupting device owner has the responsibility to initiate the review because the owner is in the best position to be aware of the operation. Manual intervention is included as a condition that initiates a review. Occasionally, Protection System failures do not yield other Protection System operations and manual intervention is required to isolate the problematic equipment. The 120 calendar day period accounts for the sporadic volumes of Protection System operations, and provides the opportunity to identify any Misoperations which were initially missed.

**R2.** Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, notify the other owner(s) of the Protection System of the operation when: *[Violation Risk Factor: Medium][Time Horizon: Operations Assessment, Operations Planning]*

**2.1** The BES interrupting device owner shares the Composite Protection System ownership with any other entity; and

**2.2** The BES interrupting device owner determined that a Misoperation occurred or cannot rule out a Misoperation; and

**2.3** The BES interrupting device owner determined that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation.

**M2.** Acceptable evidence for Requirement R2, including Parts 2.1, 2.2, and 2.3 may include, but is not limited to, the following dated documentation (electronic or hardcopy format): emails, facsimiles, or transmittals.

**Rationale for R2:** This requirement ensures that the BES interrupting device owner notifies the other owners of the Composite Protection System when the criteria in all three Parts (2.1, 2.2, and 2.3) are met, within the same 120 calendar day period as R1. This ensures other entities are notified to review their Protection System components. The expectation is that entities will communicate accordingly and when it is clear that the three conditions are met, the entity would make the notification. It is not intended for entities to automatically and unnecessarily notify other entities before adequate detail is known.

~~**Rationale for R2:** A formal CAP is a proven tool for resolving operational problems. Based on industry experience and operational coordination timeframes, the SDT believes 60 calendar days is reasonable for considering such things as alternative solutions, coordination of resources, or development of a schedule for a CAP. When the cause of a Misoperation is determined from implementing an action plan in accordance with Requirement R4, a CAP must be developed in accordance with Requirement R2.~~

~~In rare cases, altering the Protection System to avoid a Misoperation recurrence may lower the reliability or performance of the BES. In those cases, documenting the reasons for taking no corrective actions is essential for justifying the close of the Misoperation investigation process and for future reference.~~

**R3.** Each Transmission Owner, Generator Owner, ~~or~~and Distribution Provider that receives notification, pursuant to Requirement R2, within the later of 60 calendar days of notification or 120 calendar days of the BES interrupting device(s) operation, shall identify whether its Protection System component(s) caused a Misoperation. *[Violation Risk Factor: Medium][Time Horizon: Operations Assessment, Operations Planning]*

**M3.** Acceptable evidence for Requirement R3 may include, but is not limited to, the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

~~**Rationale for R3:** Where a Misoperation cause is not determined during the initial investigation; implementing an action plan of additional investigation/monitoring may determine a cause and lead to the development of a CAP in accordance with Requirement R2. The 180 calendar day period is the sum of 120 calendar days (investigative period in Requirement R1) and a 60 calendar day period (similar timeframe as in Requirement R2 for developing a CAP.)~~

~~If the action plan completion does not provide direction for identifying the cause, then pursuing further action is not warranted. In these cases, documenting the reasons is essential for justifying the close of the Misoperation investigation process and for future reference.~~

**Rationale for R3:** When an entity receives notification of a Protection System operation by the BES interrupting device owner, the Protection System owner is allotted at least 60 calendar days to identify whether it was a Misoperation. A shorter time period is allotted on the basis that the BES interrupting device owner has already performed preliminary work, collaborated with the other owners, and that other owners generally have fewer associated Protection System components.

**R4.** Each Transmission Owner, Generator Owner, and Distribution Provider that has not determined the cause(s) of a Misoperation identified in accordance with Requirement R1 or R3 shall perform investigative action(s) to determine the cause of the Misoperation at least once every two full calendar quarters after the Misoperation was first identified, until one of the following completes the investigation: *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment, Operations Planning]*

- The identification of the cause(s) of the Misoperation; or
- A declaration that no cause was identified.

**M4.** Acceptable evidence for Requirement R4 may include, but is not limited to, the following dated documentation (electronic or hardcopy format): reports, databases, spreadsheets, emails, facsimiles, lists, logs, records, declarations, analyses of sequence of events, relay targets, Disturbance Monitoring Equipment (DME) records, test results, or transmittals.

**Rationale for R4:** If a Misoperation cause is not identified within the time period established by Requirements R1 or R3 (120 calendar days), the Protection System component owner must demonstrate investigative actions toward identifying the cause(s). Performing at least one action every two full calendar quarters from first identifying the Misoperation encourages periodic focus on finding the cause of the Misoperation.

**R5.** Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the Misoperation shall, within 60 calendar days of first identifying ~~the~~a cause of ~~each~~the Misoperation: [*Violation Risk Factor: Medium*] [*Time Horizon: Operations Planning, Long-Term Planning*]

- Develop a Corrective Action Plan (CAP) for the identified Protection System component(s~~) that includes~~), and an evaluation of the CAP's applicability to the entity's other Protection Systems ~~at~~including other locations, or
- Explain in a declaration why corrective actions are beyond the entity's control or would ~~reduce~~not improve BES reliability, and that no further corrective actions will be taken.

~~**M2**~~**M5.** Acceptable evidence for Requirement R5 may include, but is not limited to, the following documentation (electronic or hardcopy format): a dated CAP or a dated declaration.

**Rationale for R5:** A formal CAP is a proven tool for resolving and reducing the possibility of reoccurrence of operational problems. A time period of 60 calendar days is based on industry experience and operational coordination time needed for considering such things as alternative solutions, coordination of resources, or development of a schedule. When the cause of a Misoperation is identified, a CAP will generally be developed. In rare cases, altering the Protection System to avoid a Misoperation recurrence may lower the reliability or performance of the BES. In those cases, a statement documenting the reasons for taking no corrective actions is essential for justifying the close of the Misoperation in lieu of a CAP and for future reference.

**R6.** Each Transmission Owner, Generator Owner, and Distribution Provider shall ~~have evidence for Requirement R2 that must include a dated CAP or a dated declaration explaining why there is no need to develop a CAP.~~

~~Each Transmission Owner, Generator Owner, or Distribution Provider shall, within 180 calendar days of the associated BES interrupting device operation, complete for each Misoperation without an identified cause:~~implement each CAP developed in Requirement R5, and update each CAP if actions or timetables change, until completed. *[Violation Risk Factor: Medium~~] [~~]][Time Horizon: Operations Planning, Long-Term Planning]*

- ~~Development of an action plan that identifies any additional investigative actions and/or Protection System modifications, including a work timetable, or~~
- ~~A declaration explaining why no further actions will be taken.~~

~~**M3.** Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence for Requirement R3 that must include a dated action plan or a dated declaration.~~

**R1.** Each Transmission Owner, Generator Owner, or Distribution Provider shall implement each CAP or action plan, and revise as needed through completion. [*Violation Risk Factor: High] [Time Horizon: Operations Planning, Long-Term Planning]*

**M4.** Each Transmission Owner, Generator Owner, and Distribution Provider shall have**M6.** Acceptable evidence for Requirement R4 that mustR6 may include, but is not limited to, dated the following documentation (electronic or hard copy format): dated records whichthat document the implementation of each CAP and action plan and the completion of actions for each CAP or action plan. The evidence. Evidence may also include dated work management program records, dated work orders, or datedand maintenance records.

**Rationale for R4**: The CAP or action plan must be completed to accomplish all identified objectives. During the course of implementing a CAP or action plan, revisions may be necessary for a variety of reasons such as scheduling conflicts or resource issues. Documenting the CAP or action plan provides auditable progress and completion confirmation on any plan. When the cause of a Misoperation is determined from implementing an action plan, a CAP must be developed in accordance with Requirement R2.

**Rationale for R6:** The CAP must accomplish all identified objectives to be complete. During the course of implementing a CAP, updates may be necessary for a variety of reasons such as new information, scheduling conflicts, or resource issues. Documenting changes or completion of CAP activities provides measurable progress and confirmation of completion.

## C. Compliance

### 1. Compliance Monitoring Process

#### 1.1. Compliance Enforcement Authority ~~(CEA)~~

As defined in the NERC Rules of Procedure, "Compliance Enforcement Authority" (CEA) means NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

#### 1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Transmission Owner, Generator Owner, and Distribution Provider ~~that owns a BES Protection System~~ shall keep data or evidence to show compliance ~~with Requirements R1, R2, R3, and R4 and Measures M1, M2, M3, and M4, since the last audit~~as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation.

- The Transmission Owner, Generator Owner, and Distribution Provider ~~that owns a BES Protection System~~ shall retain evidence of Requirements R1, R2, R3, and R4, Measures M1, M2, M3, and M4 for ~~all Misoperations with an open investigation, action plan, or~~ 12 calendar months.
- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R5, Measure M5 for 12 calendar months following completion of each CAP ~~even if the BES interrupting device operation occurred prior to the current audit period~~, evaluation, and declaration.
- The Transmission Owner, Generator Owner, and Distribution Provider shall retain evidence of Requirement R6, Measure M6 for 12 calendar months following completion of each CAP.

If a Transmission Owner, Generator Owner ~~and~~, or Distribution Provider ~~that owns a BES Protection System~~ is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved, or for the time specified above, whichever is longer.

The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

### 1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

Periodic Data Submittal

### 1.4. Additional Compliance Information

None.

## Table of Compliance Elements

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| **R1** | Operations Assessment, Operations Planning | Medium | The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 120 calendar days and less than or equal to 150 calendar days of the BES interrupting device operation. | The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 150 calendar days and less than or equal to 165 calendar days of the BES interrupting device operation. | The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 165 calendar days and less than or equal to 180 calendar days of the BES interrupting device operation. | The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1, but in more than 180 calendar days of the BES interrupting device operation.<br>OR<br>The responsible entity failed to identify whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R1. |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| R1<br>R2 | Operations Assessment, Operations Planning | Medium | The responsible entity performednotified the actionsother owner(s) of the Protection System component(s) in accordance with Requirement R1, Parts 1.1 and 1.2 R2, but in more than 120 calendar days butand less than or equal to 150 calendar days of the operation's occurrence.<br><br>OR<br><br>The responsible entity identified a Protection System operation that operated one of its BES interrupting devices but failed to review the operation in accordance with Requirement R1, Part 1.1.<br><br>OR<br><br>The responsible entity completed its review of a Protection System operation that operated one of its BES interrupting devices in 120 calendar days and | The responsible entity performednotified the actionsother owner(s) of the Protection System component(s) in accordance with Requirement R1, Parts 1.1 and 1.2 R2, but in more than 150 calendar days butand less than or equal to 160165 calendar days of the operation's occurrenceBES interrupting device operation. | The responsible entity performednotified the actionsother owner(s) of the Protection System component(s) in accordance with Requirement R1, Parts 1.1 and 1.2 R2, but in more than 160165 calendar days butand less than or equal to 170180 calendar days of the operation's occurrenceBES interrupting device operation. | The responsible entity performed the actions notified the other owner(s) of the Protection System component(s) in accordance with Requirement R1, Parts 1.1 and 1.2 R2, but in more than 170180 calendar days of the operation's occurrenceBES interrupting device operation.<br><br>OR<br><br>The responsible entity failed to identify and review a Protection System operation that operated notify one of its BES interrupting devicesor more of the other owner(s) of the Protection System component(s) in accordance with Requirement R1, Part 1.1.<br><br>OR<br><br>The responsible entity |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| R3 | Operations Assessment, Operations Planning | Medium | The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was less than or equal to 30 calendar days late. | The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 30 calendar days and less than or equal to 45 calendar days late. | The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 45 calendar days and less than or equal to 60 calendar days late. | The responsible entity identified whether or not its Protection System component(s) caused a Misoperation in accordance with Requirement R3, but was greater than 60 calendar days late.<br>OR<br>The responsible entity failed to identify whether or not a Misoperation its Protection System component(s) occurred in accordance with Requirement R3. |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| R4 | Operations Assessment, Operations Planning | Medium | The responsible entity performed at least one investigative action in accordance with Requirement R4, but was less than or equal to one calendar quarter late. | The responsible entity performed at least one investigative action in accordance with Requirement R4, but was greater than one calendar quarter and less than or equal to two calendar quarters late. | The responsible entity performed at least one investigative action in accordance with Requirement R4, but was greater than two calendar quarters and less than or equal to three calendar quarters late. | The responsible entity performed at least one investigative action in accordance with Requirement R4, but was more than three calendar quarters late.<br>OR<br>The responsible entity failed to perform investigative action(s) in accordance with Requirement R4. |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| ~~R2~~ R5 | Operations Planning, Long-Term Planning | Medium | The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement ~~R2,~~R5, but in more than 60 calendar days ~~but~~and less than or equal to 70 calendar days ~~following the identification~~ of ~~the~~first identifying a cause of the Misoperation.<br>OR<br>(See next page) | The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement ~~R2,~~R5, but in more than 70 calendar days ~~but~~and less than or equal to 80 calendar days ~~following the identification of~~ ~~the~~first identifying a cause of the Misoperation.<br>OR<br>(See next page) | The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement ~~R2,~~R5, but in more than 80 calendar days ~~but~~and less than or equal to 90 calendar days ~~following the identification~~ of ~~the~~first identifying a cause of the Misoperation.<br>OR<br>(See next page) | The responsible entity developed a CAP, or explained in a declaration in accordance with Requirement ~~R2,~~R5, but in more than 90 calendar days ~~following the identification~~ of ~~the~~first identifying a cause of the Misoperation.<br>OR<br>The responsible entity failed to develop a CAP or ~~make~~explain in a declaration in accordance with Requirement ~~R2.~~R5.<br>OR<br>(See next page) |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| R3 R5 | Operations Planning, Long-Term Planning(Continued) | Medium | The responsible entity developed an action plan, or made a declarationevaluation in accordance with Requirement R3,R5, but in more than 1860 calendar days butand less than or equal to 2170 calendar days followingof first identifying a cause of the associated BES interrupting device operationMisoperation. | The responsible entity developed an action plan, or made a declarationevaluation in accordance with Requirement R3,R5, but in more than 2170 calendar days butand less than or equal to 2280 calendar days followingfirst identifying a cause of the associated BES interrupting device operationMisoperation. | The responsible entity developed an action plan, or made a declarationevaluation in accordance with Requirement R3,R5, but in more than 2280 calendar days butand less than or equal to 2390 calendar days followingof first identifying a cause of the associated BES interrupting device operationMisoperation. | The responsible entity developed an action plan, or made a declarationevaluation in accordance with Requirement R3,R5, but in more than 2390 calendar days followingof first identifying a cause of the associated BES interrupting device operationMisoperation.<br>OR<br>The responsible entity failed to develop an action plan or a declarationevaluation in accordance with Requirement R3R5. |

| R # | Time Horizon | VRF | Violation Severity Levels | | | |
|---|---|---|---|---|---|---|
| | | | Lower VSL | Moderate VSL | High VSL | Severe VSL |
| ~~R4~~ R6 | Operations Planning, Long-Term Planning | ~~High~~Medium | The responsible entity implemented, but failed to ~~revise~~update a CAP, when actions or ~~action plan as needed~~timetables changed, in accordance with Requirement ~~R4~~R6. | N/A | N/A | The responsible entity failed to implement a CAP ~~or action plan~~ in accordance with Requirement ~~R4~~R6. |

## D. Regional Variances

None.

## E. Interpretations

None.

## F. Associated Documents

None.

## Guidelines and Technical Basis

### Introduction

This standard addresses the reliability issues identified in the letter[2] from Gerry Cauley, NERC President and CEO, dated January 7, 2011.

> "Nearly all major system failures, excluding perhaps those caused by severe weather, have misoperations of relays or automatic controls as a factor contributing to the propagation of the failure. …Relays can misoperate, either operate when not needed or fail to operate when needed, for a number of reasons. First, the device could experience an internal failure – but this is rare. Most commonly, relays fail to operate correctly due to incorrect settings, improper coordination (of timing and set points) with other devices, ineffective maintenance and testing, or failure of communications channels or power supplies. Preventable errors can be introduced by field personnel and their supervisors or more programmatically by the organization."

The standard also addresses the findings in the 2011 Risk Assessment of Reliability Performance[3]; July 2011.

> "…a number of multiple outage events were initiated by protection system Misoperations. These events, which go beyond their design expectations and operating procedures, represent a tangible threat to reliability. A deeper review of the root causes of dependent and common mode events, which include three or more automatic outages, is a high priority for NERC and the industry."

~~The composite Protection System in the context of this standard is the total complement of protection for a system Element. All protection for a given Element such as primary, secondary, backup, pilot and non-pilot relay schemes are included in the composite Protection System for the Element. These individual schemes or systems may be isolated or function independently, but aggregate as part of one composite Protection System.~~

~~A Protection System~~

### Definitions

The Misoperation definition is based on the IEEE/PSRC Working Group I3 "Transmission Protective Relay System Performance Measuring Methodology[4]." Misoperations of a Protection System include failure to operate, slowness in operating, or operating when not required either during a Fault or non-Fault condition.

[2] http://www.nerc.com/news_pr.php?npr=723[2]
http://www.nerc.com/pa/Stand/Project%20201005%20Protection%20System%20Misoperations%20DL/20110209130708-Cauley%20letter.pdf
[3] http://www.nerc.com/files/2011_RARPR_FINAL.pdf
[4] "Transmission Protective Relay System Performance Measuring Methodology," Working Group I3 of Power System Relaying Committee of IEEE Power Engineering Society, 1999.

For reference, a "Protection System" is defined in the ~~NERC~~ *Glossary of Terms* ~~as:~~ *used in NERC Reliability Standards* ("NERC Glossary") as:

- ~~•~~ Protective relays which respond to electrical quantities,
- ~~•~~ Communications systems necessary for correct operation of protective functions,
- ~~•~~ Voltage and current sensing devices providing inputs to protective relays,
- ~~•~~ Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply), and
- ~~•~~ Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.

~~Circuit breaker and other~~A BES interrupting device is a BES Element, typically a circuit breaker or circuit switcher that has the capability to interrupt fault current. Although BES interrupting device mechanisms are not part of a Protection System~~.~~

~~A revised~~ , the standard uses the operation of a BES interrupting device by a Protection System to initiate the review for Misoperation ~~definition is~~ .

The following two definitions are being proposed for ~~industry adoption;~~inclusion in the ~~failure~~ NERC Glossary:

> **Composite Protection System –** *The total complement of* ~~an Element's~~*the Protection System(s) that function collectively to protect a Element, such as any primary, secondary, local backup, and communication-assisted relay systems. Backup protection provided by a remote Protection System is excluded.*

This definition has been introduced in this standard and incorporated into the proposed definition of Misoperation to clarify that the entity must consider the entire Protection System associated with the BES interrupting device that operated. Additionally, the definition accounts for those Protection Systems with multiple levels of protection (e.g., redundant systems), such that if one component fails, but the overall intended performance of the composite protection is met – it would not be identified as a Misoperation under the definition.

> **Misoperation –** *The failure a Composite Protection System to operate as intended.* ~~The definition includes~~*Any of the following* ~~categories~~*is a Misoperation:*
>
> 1. ~~(1)~~**Failure to Trip – During Fault –** *A failure of a Composite Protection System to operate for a Fault* ~~**within the zone**~~*condition for which it is designed* ~~**to protect.**~~ *. The failure of a Protection System component is not a Misoperation as long as the* ~~**overall**~~ *performance of the Composite Protection System is correct.*
>
> ***Failure to Trip – Other Than Fault** – A failure of a Composite Protection System to operate for* ~~**the Element**~~*a non-Fault condition for which it is designed* ~~**to protect is correct.**~~

2. ~~A failure of a transformer's composite Protection System to operate for a transformer Fault is an example of a "~~*, such as a power swing, undervoltage, overexcitation, or loss of excitation. The failure* ~~to trip" Misoperation. This type~~*of a Protection System component is not a Misoperation as long as the performance of the Composite Protection System is correct.*

3. ***Slow Trip – During Fault*** *– A Composite Protection System operation that is slower than required for a Fault condition for which it is designed. Delayed clearing of a Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or resulted in the operation of any other Composite Protection System.*

4. ***Slow Trip – Other Than Fault*** *– A Composite Protection System operation that is slower than required for a non-Fault condition for which it is designed, such as a power swing, undervoltage, overexcitation, or loss of excitation. Delayed clearing of a non-Fault condition is a Misoperation if high-speed performance was previously identified as being necessary to prevent voltage or dynamic instability, or resulted in the operation of any other Composite Protection System.*

5. ***Unnecessary Trip – During Fault*** *– An unnecessary Protection System operation for a Fault condition on another Element.*

6. ***Unnecessary Trip – Other Than Fault*** *– An unnecessary Protection System operation for a non-Fault condition for which it is not designed. A Protection System operation that is caused by on-site maintenance, testing, inspection, construction or commissioning activities is not a Misoperation.*

Failure to automatically reclose after a Fault condition is not included as a Misoperation because reclosing equipment is not included within the definition of Protection System.

This proposed definition of Misoperation provides additional clarity over the current version. A Misoperation is the failure of a Composite Protection System to operate as intended. The definition includes six categories which provide further differentiation and examples of what is a Misoperation. These categories are discussed in greater detail in the following sections.

## Failure to Trip – During Fault

This category of Misoperation typically results in the Fault condition being cleared by remote backup Protection System operation~~s~~.

**Example 1a:** A failure of a transformer's Composite Protection System to operate for a transformer Fault is a Misoperation.

**Example 1b:** A failure of a "primary" transformer relay (or any other component) to operate for a transformer Fault is not a ~~"failure to trip"~~ Misoperation as long as another component of the transformer's ~~c~~Composite Protection System operated to clear the Fault~~. Please see category 3 to see if the "slow trip" classification applies to the operation~~.

**Example 1c:** A lack of target information~~, e.g. when~~ does not by itself constitute a Misoperation. When a high-speed pilot system does not target because a high-speed zone element trips first~~, does~~ would not ~~by~~in and of itself ~~constitute~~be a Misoperation.

**~~(2) A failure of a Protection System to operate for a non-Fault condition for which~~**In analyzing the Protection System **~~was intended to operate, such as a power swing, under-voltage, over excitation, or loss of excitation. The failure of a Protection System component is not a Misoperation as long as the overall performance of the Protection System for the Element it is designed to protect is correct.~~**

~~A failure of a generator's composite Protection System to operate for a loss of field condition is an example of a "failure to trip"~~ for Misoperation~~. This type of Misoperation may require manual operator intervention.~~

~~A failure of a "primary" reverse power relay (or any other component) is not a "failure to trip" Misoperation as long as another component of the generator's composite Protection System operated to shut down the generator. Please see~~, the entity must also consider whether the "Slow Trip – During Fault" category ~~4 to see if the "slow trip" classification~~ applies to the operation.

~~The non-~~

## Failure to Trip – Other Than Fault

This category of Misoperation may have resulted in operator intervention. The "Failure to Trip – Other Than Fault" conditions cited in the definition are examples only, and do not constitute an all-inclusive list.

**~~(3) A Protection System operation that is slower than intended for a Fault within the zone it is designed to protect. Delayed Fault clearing associated with an installed high-speed protection scheme is not a Misoperation if the high-speed performance has not been identified to meet the dynamic stability performance requirements of the TPL standards nor is it required to ensure coordination with other Protection Systems.~~**

~~A failure of a line's composite Protection System to operate as quickly as intended for a line Fault is an example of a "slow trip"~~ **Example 2a:** A failure of a generator's Composite Protection System to operate for an unintentional loss of field condition is a Misoperation.

**Example 2b:** A failure of an overexcitation relay (or any other component) is not a "Failure to Trip – Other Than Fault" Misoperation as long as another component of the generator's Composite Protection System operated as intended (e.g., isolating the generator).

In analyzing the Protection System for Misoperation~~.~~, the entity must also consider whether the "Slow Trip – Other Than Fault" category applies to the operation.

## Slow Trip – During Fault

This ~~type~~category of Misoperation typically results in remote backup Protection System operation~~s~~ before the Fault is cleared.

> ~~In many cases,~~**Example 3:** A failure of a line's Composite Protection System to operate as quickly as intended for a line Fault is a Misoperation.

Installing high-speed protection ~~is installed as~~ may be a part of ~~the~~a utility's standard practice without having the need for high-speed protection ~~for meeting TPL requirements. A slow trip of this Protection System~~to prevent voltage or dynamic instability or to maintain relay coordination. For this case, a "Slow Trip – During Fault" of the high-speed protection is not a Misoperation because it would not negatively impact the dynamic ~~performance of the BES; so, it does not need to be reported. However, even if high-speed clearing is not required, the~~BES performance, unless the Composite Protection System operation is slower than previously identified as being necessary to prevent voltage or dynamic instability. The Composite Protection System must also coordinate with other Protection Systems to prevent the trip (e.g., an over-trip) of additional Protection Systems ~~must coordinate to prevent an "unnecessary trip" Misoperation (e.g. an over trip).~~.

The phrase "slower than ~~intended~~required" means the Composite Protection System operated slower than the objective of the owner(s). It would be ~~impossible~~impractical to provide a precise tolerance in the definition that would be applicable to every type of Protection System. Rather, the owner(s) reviewing each Protection System operation should ~~have an understanding of the objectives of its Protection Systems, whether those systems operated fast enough to prevent additional harm, and ultimately be able to decide~~understand whether the speed ~~or~~and outcome of its Protection System operation ~~was adequate~~met their objective. The intent is not to require documentation of exact Protection System operation times, but to assure consideration of relay coordination and stability by the owner(s) reviewing each Protection System operation.

The ~~reference to the TPL standards is meant to place some bounds on the time to clear a Fault and prevent dynamic instability. The performance requirements~~phrase "resulted in the ~~TPL standards are found in Table 1, and are applicable to all contingencies mentioned for Type A, B and C contingencies.~~

~~Coordination with~~operation of any other Composite Protection System~~s~~" refers to the need to ensure that relaying operates in the proper or planned sequence (i.e~~.~~., the primary relaying for a faulted Element operates before the remote backup relaying for the faulted Element).

~~**(4) A Protection System operation that is slower than intended for a non-Fault condition such as a power swing, under-voltage, over excitation, or loss of excitation for which it was intended to operate.**~~

~~A failure of a generator's composite Protection System to operate as quickly as intended for an over excitation condition is an example of a "slow trip" Misoperation. This type of Misoperation may result in equipment damage.~~

In analyzing the Protection System for Misoperation, the entity must also consider the "Unnecessary Trip – During Fault" category to determine if an "unnecessary trip" applies to the Protection System operation of an Element other than the faulted Element.

## Slow Trip – Other Than Fault

The phrase "slower than ~~intended~~required" means the ~~c~~Composite Protection System operated slower than the objective of the owner(s). It would be ~~impossible~~impractical to provide a precise tolerance in the definition that would be applicable to every type of Protection System. Rather, the owner(s) reviewing each Protection System operation should ~~have an understanding of the objectives of its Protection Systems, whether those systems operated fast enough to prevent additional harm, and ultimately be able to decide~~understand whether the speed ~~or~~and outcome of its Protection System ~~was adequate~~operation met their objective. The intent is not to require documentation of exact Protection System operation times, but to assure consideration of relay coordination and stability by the owner(s) reviewing each Protection System operation.

> **Example 4:** A failure of a generator's Composite Protection System to operate as quickly as intended for an overexcitation condition is a Misoperation. This category of Misoperation could result in equipment damage.

The ~~non-~~"Slow Trip – Other Than Fault" conditions cited in the definition are examples only, and do not constitute an all-inclusive list.

**~~(5) A Protection System operation for a Fault for which the Protection System is not intended to operate.~~**

~~An operation of a transformer's composite Protection System which over trips for a properly cleared line Fault is an example of an "unnecessary trip" Misoperation. For this type of Misoperation, the Fault is typically cleared properly by the faulted equipment's composite Protection System (line relaying, in this case) without the need for an external Protection System's operation.~~

## Unnecessary Trip – During Fault

An operation of a properly coordinated remote Protection System~~s~~ is not in and of itself a Misoperation if the Fault has persisted for a sufficient time to allow the correct operation of the ~~local~~Composite Protection System of the Faulted Element to clear the Fault. ~~An~~A BES interrupting device failure, a "failure to trip" Misoperation, or a "slow trip" Misoperation may result in a proper remote Protection System operation.

**~~(6) A Protection System operation for a non-Fault condition for which the Protection System is not intended to operate, and is unrelated to on-site maintenance, testing, inspection, construction or commissioning activities.~~**

> ~~Non-Fault~~ **Example 5:** An operation of a transformer's Composite Protection System which trips (i.e., over-trips) for a properly cleared line Fault is a Misoperation. The Fault is cleared properly by the faulted equipment's Composite Protection System (i.e., line relaying) without the need for an external Protection System operation resulting in an unnecessary trip of the transformer protection; therefore, the transformer Protection System operation is a Misoperation.

## Unnecessary Trip – Other Than Fault

Unnecessary trips for non-Fault conditions include but are not limited to, power swings, ~~over excitation~~overexcitation, loss of excitation, frequency excursions, and normal ~~c~~o~~ndi~~perations.

> **Example 6a:** An operation of a line's ~~c~~Composite Protection System due to a relay failure during normal ~~conditions is an example of an "unnecessary trip other than Fault"~~operation is a Misoperation.
>
> ~~In a second example, tripping~~**Example 6b:** Tripping a generator by the operation of the loss of field protection during an off-nominal frequency condition while the field is intact is a Misoperation~~. In a third example, an~~ assuming the Composite Protection System was not intended to operate under this condition.
>
> **Example 6c:** An impedance line relay trip for a power swing that entered the relay's characteristic is a Misoperation if the power swing was stable and the relay operated because ~~it was set with an excessive reach that unnecessarily restricted the line's load carrying capability~~power swing blocking was enabled and should have prevented the trip, but did not.

~~An~~Additionally, an operation that occurs during a non-~~f~~Fault condition but was initiated directly by on-site (i.e., real-time) maintenance, testing, inspection, construction, or commissioning is not a Misoperation. ~~However~~

> **Example 6d:** A BES interrupting device operation that occurs at the remote end of a line during a non-Fault condition because a direct transfer trip was initiated by system maintenance and testing activities at the local end of the line is not a Misoperation.

The "on-site" activities at one location that initiates a trip to another location are included in this exemption; however, once the maintenance, testing, inspection, construction, or commissioning ~~has been completed~~is complete, the "on-site" Misoperation exclusion no longer applies, regardless of the presence of ~~the technical~~on-site personnel.

## Special Cases

Protection System operations for these cases would not be a Misoperation.

> **Example 7a:** A generator Protection System operation prior to closing the unit breaker(s) is not a Misoperation provided no in-service Elements are tripped.

This type of operation is not a Misoperation because the generating unit is not synchronized and is isolated from the BES. Protection System operations which occur with the protected Element out of service, that do not trip any in-service Elements, are not Misoperations.

In some cases where zones of protection overlap, the owner(s) of Elements may decide to allow a Protection System to operate faster in order to gain better overall Protection System performance for an Element.

**Example 7b:** The high-side of a transformer connected to a line may be within the zone of protection of the supplying line's relaying. In this case, the line relaying is planned to protect the area of the high side of the transformer and into its primary winding. ~~This definition is based on the established IEEE/PSRC I3 Working Group on 'Transmission Protective Relay System~~

~~Performance Measuring Methodology' categories (excluding Failure to Reclose) of Relay System Misoperation. The phrase abnormal condition has been replaced with "non-fault condition" to remove ambiguity.~~

~~The exclusion of a component failure, as long as the composite Protection System operates correctly, was based on recommendations by the NERC SPCS. Entities still need to review each Protection System operation. Covering these types of component failures within the standard constitutes additional administrative burden for types of failures that have no immediate reliability impacts.~~

~~Failure to automatically reclose after a Fault is not included as a Misoperation because reclosing equipment is not included under the definition of Protection Systems.~~

> In order to provide faster protection for the line, the line relaying may be designed and set to operate without direct coordination (or coordination is waived) with local protection for Faults on the high-side of the connected transformer. Therefore, the operation of the line relaying for a high-side transformer Fault operated as intended and would not be a Misoperation.

The above are examples only, and do not constitute an all-inclusive list of conditions that would not be a Misoperation.

## Non-Protective Functions

BES interrupting device operations which are initiated by non-protective functions, such as those associated with generator controls, excitation controls, or turbine/boiler controls, ~~Static VAR Compensators (SVCs), Flexible AC Transmission Systems~~static voltampere-reactive compensators (SVC), flexible ac transmission systems (FACTS), ~~High Voltage DC (HVDC~~high-voltage dc (HVdc) transmission systems, circuit breaker mechanisms, or other facility control systems are not operations of a Protection System. ~~Additionally, operations initiated by control functions within protective relays are not considered Protection System operations. For example, in cases where a component of the Protection System or a function of a component within the Protection System is used for control of a generator, such as when a reverse power relay is used to trip a breaker during generator shutdown, the operation of the control component or the function when not providing protection is not included in the definition of Misoperation and its operation would not be reviewed under this standard. Automation (e.g. data collection) is also not a protective function and is not subject to this standard~~ The standard is not applicable to non-protective functions such as automation (e.g., data collection) or control functions that are embedded within a Protection System.

~~A generator Protection System operation prior to closing the unit breaker(s) is not considered a Misoperation provided no in-service BES Elements are tripped. These types of operations are excluded when the generating unit is not synchronized and is isolated from the BES. Protection System operations which occur with the protected Element out-of-service, that do not trip any in-service Elements are not Misoperations. Protection System operations unrelated to on-site maintenance, testing, inspection, construction or commissioning activities which occur with the protected Element out-of-service, that trip any in-service Elements are Misoperations.~~

~~In some cases where zones of protection overlap, the owner of BES Elements may decide to allow a Protection System to operate faster in order to gain better overall Protection System~~

performance for an Element. For example, the high side of a transformer connected to a line may be within the zone of protection of the supplying line's relaying. In this case, the line relaying is planned to protect the area of the high side of the transformer and into its primary winding. In order to provide faster protection for the line, the line relaying may be designed and set to operate without direct coordination (or coordination is waived) with local protection for Faults on the high side of the connected transformer. Therefore, the operation of the line relaying for a high side transformer Fault would not be considered a Misoperation.

> This standard addresses the reliability issues identified in the letter[5] from Gerry Cauley, NERC President and CEO, dated January 7, 2011. "Nearly all major system failures include misoperation of relays as a factor contributing to the propagation of the events…….. Reducing the risk to reliability from relay Misoperations requires consistent collection of misoperation information by regional entities, along with systematic analysis and correction of the underlying causes of preventable Misoperations." The standard also addresses the findings in the 2011 Risk Assessment of Reliability Performance[6]; July 2011 "….a number of multiple outage events were initiated by protection system Misoperations. These events, which go beyond their design expectations and operating procedures, represent a tangible threat to reliability. A deeper review of the root causes of dependent and common mode events, which include three or more automatic outages, is a high priority for NERC and the industry."

## Control Functions

The entity must make a determination as to whether the standard is applicable to its Protection System in accordance with the provided exclusions in the standard's Applicability, see Section 4.2.1. The subject matter experts (SME) developing this standard recognize that entities use Protection Systems as part of a routine practice to control BES Elements. This standard is not applicable to protective functions within a Protection System when intended for controlling a BES Element as a part of an entity's process or planned switching sequence. The following are examples of conditions to which this standard is not applicable:

> **Example 8a:** The reverse power protective function that operates to remove a generating unit from service using the entity's normal or routine process.
>
> **Example 8b:** The reverse power relay enables a permissive trip and the generator operator trips the unit.

In the example above, the standard is not applicable; however, the standard remains applicable to the reverse power relay as a part of the generator Protection System when intended to provide generator anti-motoring protection. For example, reverse power relays are typically installed as the primary protection for a generating unit to guard against motoring. Though, operators often take advantage of this functionality and use the Protection System's reverse power protective function as a normal procedure to shutdown a generating unit.

---

[5] http://www.nerc.com/news_pr.php?npr=723[5] http://www.nerc.com/pa/Stand/Project%20201005%20Protection%20System%20Misoperations%20DL/20110209130708_Cauley%20letter.pdf

[6] http://www.nerc.com/files/2011_RARPR_FINAL.pdf

The following is another example of a condition to which this standard is not applicable:

> **Example 8c:** Operation of a capacitor bank interrupting device for voltage control using functions embedded within a microprocessor based relay that is part of a Protection System.

The above are examples only, and do not constitute an all-inclusive list to which the standard is not applicable.

## Extenuating Circumstances

In the event of a natural disaster~~, note that the~~ or other extenuating circumstances, the December 20, 2012 Sanction Guidelines of the North American Electric Reliability Corporation ~~effective January 15, 2008 provides that the Compliance Monitor~~, Section 2.8, Extenuating Circumstances, says: "In unique extenuating circumstances causing or contributing to the violation, such as significant natural disasters, NERC or the Regional Entity may significantly reduce or eliminate Penalties." The Regional Entities to whom NERC has delegated authority will consider extenuating circumstances when considering any sanctions in relation to the timelines outlined in this standard.

~~**Requirement R1**~~

~~This requirement promotes the prudent evaluation of each Protection System operation to determine if the operation was correct or a Misoperation, even those Misoperations difficult to detect. Unless all BES Protection System operations and Faults that challenge them are reviewed, it cannot be determined with certainty that all Misoperations are identified. For example, if you only reviewed operations resulting in an overtrip, you would not necessarily identify Misoperations caused by slow trips.~~

~~Requirement R1 places the responsibility on~~ The volume of Protection System operations tend to be sporadic. If a high rate of Protection System operations is not sustained, utilities will have an opportunity to catch up within the 120 day period.

## Requirement R1

This requirement initiates a review of each BES interrupting device operation to identify whether or not a Misoperation may have occurred. Since the BES interrupting device owner ~~to investigate~~ typically monitors and tracks device operations ~~initiated by a Protection System. The drafting team believes,~~ the owner is the logical starting point for identifying Misoperations of ~~the~~Protection Systems for BES ~~interrupting device that operated would be in the best position to analyze the Protection System operation, determine if a Misoperation occurred, and perform the initial investigation to determine the cause of the Misoperation. If the~~ Elements. A review is required when (1) a BES interrupting device ~~owner does not own all of the~~ operates that is caused by a Protection System ~~and cannot determine that the~~or by manual intervention in response to a Protection System ~~operation was correct, then notify~~failure to operate, (2) regardless of whether the ~~other~~ owner~~(s)~~ owns all or part of the Protection System component(s), and (3) the owner identified that its Protection System component(s) ~~and provide~~as causing the BES interrupting device operation.

Since most Misoperations result in the operation of one or more BES interrupting devices, these operations initiate a review to identify any ~~requested investigative information. In this case, it is expected that both entities will work together to investigate the cause of the operation~~Misoperation. If an Element is manually isolated in response to a failure to operate, the manual isolation of the Element triggers a review for Misoperation.

> **Example R1a:** The failure of a loss of field relay on a generating unit where an operator takes action to isolate the unit.

Manual intervention may indicate a Misoperation has occurred, thus requiring the initiation of an investigation by the BES interrupting device owner.

Protection Systems are made of many components. These components may be owned by ~~more than one entity.~~different entities. For example, a Generator Owner may own a current transformer that sends information to a Transmission Owner's differential relay. All of these components and many more are part of a Protection System. It is expected that all of the owners will communicate with each other, sharing ~~any~~ information freely, so that Protection System operations can be analyzed, Misoperations identified, and corrective actions taken~~. If an entity feels it cannot get the level of cooperation it needs to adequately address a Misoperation, the entity should appeal to its Regional Entity for help in resolving the situation~~.

~~Determining~~Each entity is expected to use judgment to identify those Protection System operations that meet the definition of Misoperation regardless of the level of ownership. A combination of available information from resources such as counters, relay targets, Supervisory Control and Data Acquisition (SCADA) systems, or Disturbance Monitoring Equipment (DME) would typically be used to determine whether or not a Misoperation occurred. The entity is allotted 120 calendar days from the date of its BES interrupting device operation to identify whether or not a Misoperation of its Protection System component(s) occurred.

The Protection System operation may be documented in a variety of ways such as in a report, database, spreadsheet, or list. The documentation may be organized in a variety of ways such as by BES interrupting device, protected Element, or Composite Protection System.

## Requirement R2

For Requirement R2 (i.e., case of multi-entity ownership), the entity that owns the BES interrupting device that operated is expected to use judgment to identify those Protection System operations that meet the definition of Misoperation under Requirement R1; however, if the entity that owns a BES interrupting device determines that its Protection System component(s) did not cause the BES interrupting device(s) operation or cannot determine whether its Protection System components caused the BES interrupting device(s) operation, it must notify the other Protection System owner(s) when the criteria in Requirement R2 is met.

This requirement does not preclude the Protection System owners from initially communicating and working together to determine whether a Misoperation occurred and, if so, the cause. The BES interrupting device owner is only required to officially notify the other owners when it: (1) shares the Composite Protection System ownership with other entity(ies), (2) determines that a Misoperation occurred or cannot rule out a Misoperation, and (3) determines its Protection System component(s) did not cause a Misoperation or is unsure. Officially notifying the other owners without performing a preliminary review may unnecessarily burden the other owners

with compliance obligations, redirect valuable resources, and add little benefit to reliability. The BES interrupting device owner should officially notify other owners when appropriate within the established time period.

The following is an example of a notification to another Protection System owner:

> **Example R2a:** Circuit breakers A and B at the Charlie station tripped from directional comparison blocking or DCB relaying on 03/03/2014 at 15:43 UTC during an external fault. As discussed last week, the fault records indicate that a problem with your equipment (failure to transmit) caused the operation.

## Requirement R3

For Requirement R3 (i.e., notification received), the entity that also owns a portion of the Composite Protection System is expected to use judgment to identify whether the Protection System operation is a Misoperation. A combination of available information from resources such as counters, relay targets, SCADA, DME, and information from the other owner(s) would typically be used to determine whether or not a Misoperation occurred.

The entity that is notified by the BES interrupting device owner is allotted the later of 60 calendar days from receipt of notification or 120 calendar days from the BES interrupting device operation date to determine if its portion of the Composite Protection System caused the Protection System operation. It is expected that in most cases of a jointly owned Protection System, the entity making notification would have been in communication with the other owner(s) early in the process. This means that the shorter 60 calendar days only comes into play if the notification occurs in the latter half of the 120 calendar days allotted to the BES interrupting device owner.

The Protection System review may be organized in a variety of ways such as in a report, database, spreadsheet, or list. The documentation may be organized in a variety of ways such as by BES interrupting device, protected Element, or Composite Protection System. The BES interrupting device owner's notification received may be documented in a variety of ways such an email or a facsimile.

## Requirement R4

The entity in Requirement R4 (i.e., cause identification), whether it is the entity that owns the BES interrupting device or an entity that was notified, the entity is expected to use due diligence in taking investigative action(s) to determine the cause(s) of an identified Misoperation for its portion of the Composite Protection System. The SMEs developing this standard recognize there will be cases where the cause(s) of a Misoperation will not be revealed during the allotted time periods in Requirements R1 or R3; therefore, Requirement R4 provides the entity a mechanism to continue its investigative work to determine the cause(s) of the Misoperation when the cause is not known.

A combination of available information from resources such as counters, relay targets, SCADA, DME, test results, and studies would typically be used to determine the cause of the Misoperation. At least one investigative action must be performed every two full calendar quarters until the investigation is completed.

The following is an example of investigative actions taken to determine the cause of an identified Misoperation:

> **Example R4a**: A Misoperation was identified on 03/18/2014. A line outage to test the Protection System was scheduled on 03/24/2014 for 12/15/2014 (i.e., beyond the next two full calendar quarters) due to summer peak conditions. The protection engineer contacted the manufacturer on 04/10/2014 (i.e., within two full calendar quarters) to obtain any known issues. The engineer reviewed manufacturer's documents on 05/27/2014. The outage schedule was confirmed on 08/29/2014 and was taken on 12/15/2014. Testing was completed on 12/16/2014 (i.e., in the second two full quarters) revealing the microprocessor relay as the cause of the Misoperation. A CAP is being developed to replace the relay.

Periodic action minimizes compliance burdens and focuses the entity's effort on determining the cause(s) of the Misoperation while providing measurable evidence. The SMEs recognize that certain planned investigative actions may require months to schedule and complete; therefore, the entity is only required to perform at least one investigative action every two full calendar quarters. Investigative actions may include a variety of actions, such as reviewing DME records, performing or reviewing studies, completing relay calibration or testing, requesting manufacturer review, or requesting a necessary outage.

The entity's investigation is complete when it identifies the cause of the Misoperation or makes a declaration that no cause was determined. The declaration is intended to be used if the entity determines that investigative actions have been exhausted or have not provided direction for identifying the Misoperation cause.

Although the entity only has to document its specific investigative actions taken to determine the cause(s) of an identified Misoperation, the entity should consider the benefits of formally organizing (e.g., in a report or database) its actions and findings. Well documented investigative actions and findings may be helpful in future investigations of a similar event or circumstances. A thorough report or database may contain a detailed description of the event, information gathered, investigative actions, findings, possible causes, identified causes, and conclusions. Multiple owners of a Composite Protection System might consider working together to produce a common report for their mutual benefit.

The following are examples of a declaration where no cause was determined:

> **Example R4b**: All relays at station A and B functioned properly during testing on 08/26/2014. The carrier system functioned properly during testing on 08/27/2014. The carrier coupling equipment functioned properly during testing on 08/28/2014. A settings review completed on 09/03/2014 indicated the relay settings were proper. Since the equipment involved in the operation functioned properly during testing, the settings were reviewed and found to be correct, and the equipment at station A and station B is already monitored. The investigation is being closed because no cause was found.
>
> **Example R4c:** The protection scheme was replaced before the cause was identified. The power line carrier or PLC based protection was replaced with fiber-optic based protection with an in service date of 04/16/2014. The new system will be monitored for recurrence of the Misoperation.

## Requirement R5

Resolving the causes of Protection System Misoperations ~~is essential in developing an effective remedy to avoid future Misoperations. The drafting team recognizes that~~benefits BES reliability by preventing recurrence. The Corrective Action Plan or CAP is an established tool for resolving operational problems. The NERC Glossary defines a Corrective Action Plan as, *"A list of actions and an associated timetable for implementation to remedy a specific problem."* When the Misoperation cause is identified in Requirement R1, R3 or R4, Requirement R5 requires Protection System owner(s) to develop a CAP or explain why corrective actions are beyond the entity's control or would not improve BES reliability. The entity must create the CAP or make a declaration why additional actions are beyond the entity's control or would not improve BES reliability and that no further corrective actions will be taken within 60 calendar days of first determining a cause.

The SMEs developing this standard recognize there may be multiple causes for a Misoperation; in these circumstances, the CAP would include a remedy for the identified causes. The ~~60-day clock for developing the CAP will be associated with the determination of the first cause. A CAP can~~CAP may be revised if additional causes are found~~. The drafting team believes 120 calendar days is a reasonable period of time to investigate operations, determine the cause for most Misoperations and document findings in a Misoperation investigation report. This time frame takes into account the seasonal nature of Protection System operations. Both the volume of Protection System operations as well as outage constraints for investigative purposes can be seasonal.~~

~~Regardless of whether a cause is identified, the BES interrupting device owner must document the investigation as a potential aid in possible future Misoperation investigations. If a~~; therefore, the entity has the option to create a single ~~Protection System causes~~or multiple ~~BES interrupting device owners to be affected, the entities may work together to produce a common Misoperation investigation report. Similarly, if the BES interrupting device owner and the Protection System component owner that caused a Misoperation are different entities, they may work together to produce a common report.~~

~~A Misoperation investigation report or documented findings may include the following information: 1) initial evidence, 2) probable causes, 3) tests and studies, and 4) conclusions. A brief description of the event surrounding the Misoperation may be included if not separately documented. The initial evidence, which may also be documented separately, contains the sequence of events, relay targets and a summary of Disturbance Monitoring Equipment (DME) records as appropriate. Probable causes are those causes which are most likely to have contributed to the Misoperation and could be considered for further testing. The test and studies documented in the report would describe and provide findings of those tests if the entity was able to perform them during the initial investigation phase (e.g. relay calibration and simulation tests, communication noise and attenuation tests, CT/VT ratio tests, DC continuity checks and functional tests) and studies (e.g. short circuit and coordination studies) performed in the attempt to determine the cause. The conclusions should summarize the cause(s) substantiated by the evidence and findings of the tests and studies.~~

~~**Requirement R2**~~

If the Misoperation cause is identified within 120 days of the event, Requirement R2 requires Protection System owners to develop a CAP or to make a declaration of no additional action within 60 calendar days of determining the cause. The drafting team recognizes there may be CAPs to correct multiple causes forof a Misoperation; in these circumstances the CAP would include a remedy for the identified causes. The 60 calendar day clockperiod for developing the CAP will be associated with the determination of the first cause. A a CAP can be revised if additional causes are found. Based on (or declaration) is established on the basis of industry experience and which includes operational coordination timeframes, the drafting team believes 60 calendar days is reasonable for considering such things astime to consider alternative solutions, coordination of resources, orand development of a schedule for a CAP, or to prepare a declaration justifying the lack of a CAP.

The 120 day time period and the 60 dayThe time periods within Requirement R1, R3 and Requirement R5 are distinct and separate. If a cause of a Misoperation is identified quickly, the time period are distinct and within the context ofin Requirement R1 and Requirement R2 respectively, needor R3 ends and the 60 calendar day period to remain separate. Withdevelop the CAP becomes applicable. The ultimate goal of keeping the implementationis to keep all time of a CAPperiods as short as possible, if a cause of a Misoperation is determined quickly the CAP creation timeframe (60 days) becomes applicable and requires the CAP implementation be less than 180 days. Also, if the interrupting device owner is tardy in informing another Protection System component owner and using up much of the 120 day period, it still leaves a considerable amount of time (at least 60 days) to develop an action plan for further investigation by the Protection System component owner, or if a cause is determined the creation of the CAP.

including the correction of the cause(s) of the Misoperation. Where there are multiple Protection System owners involved in a Misoperation, the one or more owners each owner whose Protection System component(s) contributed to the Misoperation will create a CAP or declaration as required by Requirement R2. Owners whose Protection System components operated correctly do not need to create a CAPis subject to Requirement R5.

Resolving Misoperations benefits the Protection System owner and the BES by maintaining reliability and security. The CAP is an established tool for resolving operational problems. The NERC Glossary of Terms defines a Corrective Action Plan as "A list of actions and an associated timetable for implementation to remedy a specific problem".

Protection System owners are expected to exercise due diligence in theThe development and implementation of a CAP. Typically included would be any is intended to document the specific corrective actions needed to be taken to prevent Misoperation recurrence (along with, the date performed), any correctivetimetable for executing such actions planned to be taken to prevent recurrence (along with the planned date),, and an evaluation of the CAP's applicability to the entity's other Protection Systems owned by the entity.

including other locations. The evaluation of the CAP's applicability to these other Protection Systems owned byaims to reduce the entity is intended to encourage diligence in preventingrisk and likelihood of similar Misoperations. in other Protection Systems. The Protection System owner is responsible for determining the scope of the problem, and for including appropriate actions in the CAP. extent of its evaluation concerning other Protection Systems and locations. The evaluation may result in adding preemptive actions to the CAP. The CAP is complete when

all specified actions are completedthe owner including actions to address Protection Systems at other locations or the reasoning for not taking any action. The CAP must include an evaluation of other Protection Systems including other locations to be complete.

The following are examplesis an example of Corrective Action Plans (CAPs):

a CAP Example 1 – Corrective actions for a failed relay only:

The impedance relay was removed from service on 6/2/12 because itMisoperation that was applying a standing trip. Relay testing was performed on 6/4/12. A due to a failed capacitor was found within the impedance relay. The and the evaluation of the cause at similar locations which determined capacitor was replaced on 6/5/12. The impedance relay functioned properly during testing after thereplacement was not necessary.

> **Example R5a:** Actions: Remove the relay from service. Replace capacitor was replaced. The impedance. Test the relay was returned. Return to service on 6/5/12or replace by 07/01/2014.
>
> Applicability to other Protection Systems: Undesired trips of this This type of impedance relay due to capacitor failures have occurred only occasionally within our system. This type of impedance relay is graduallyhas not been experiencing problems and is systematically being replaced with microprocessor relays as Protection Systems are modernized. It is therefore our assessment Therefore, it was assessed that a program for wholesale preemptive replacement of capacitors in this type of impedance relay does not need to be established for ourthe system.

CAP Example 2 – Corrective actions for a failed relay, and a program for preemptive actions at similar installations:

The impedanceThe following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor and the evaluation of the cause at similar locations which determined the capacitors need preemptive correction action.

> **Example R5b:** Actions: Remove the relay was removed from service on 6/2/12 because it was applying a standing trip. Relay testing was performed on 6/4/12. A failed capacitor was found within the impedance relay. The. Replace capacitor was replaced on 6/5/12. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned. Test the relay. Return to service on 6/5/12or replace by 07/01/2014.
>
> Applicability to other Protection Systems: Undesired trips of thisThis type of impedance relay dueis suspected to capacitor failures have occurred frequently. It is therefore our assessment that previously tripped at other locations because of the same type of capacitor issue. Based on the evaluation, a program should be established by 12/1/1201/2014 for wholesale preemptive replacement of capacitors in this type of impedance relay.

The following is an example of a CAP for a relay Misoperation that was applying a standing trip due to a failed capacitor and the evaluation of the cause at similar locations which determined the capacitors need preemptive correction action.

**Example R5c:** Actions: Remove the relay from service. Replace capacitor. Test the relay. Return to service or replace by 07/01/2014.

Applicability to other Protection Systems: This type of impedance relay is suspected to have previously tripped at other locations because of the same type of capacitor issue. Based on the evaluation, the preemptive replacement of capacitors in this type of impedance relay should be pursued for the identified stations A through I by 04/30/2015.

A plan is being developed to replace the impedance relay capacitors at stations A, B, and C by 09/01/2014. A second plan is being developed to replace the impedance relay capacitors at stations D, E, and F by 11/01/2014. The last plan will replace the impedance relay capacitors at stations G, H, and I by 02/01/2015.

The following is an example of a CAP for a relay Misoperation that was due to a version 2 firmware problem and the evaluation of the cause at similar locations which determined the firmware needs preemptive correction action.

**Example R5d:** Actions: Provide the manufacturer Fault records. Install new firmware pending manufacturer results by 10/01/2014.

Applicability to other Protection Systems: Based on the evaluation of other locations and a risk assessment, the newer firmware version 3 should be installed at all installations that are identified to be version 2. Twelve relays were identified across the system. Proposed completion date is 12/31/2014.

The following are examples of a declaration made where corrective actions are beyond the entity's control or would not improve BES reliability and that no further corrective actions will be taken.

**Example R5e:** The cause of the Misoperation was due to a non-registered entity communications provider problem.

**Example R5f:** The cause of the Misoperation was due to a transmission transformer tapped industrial customer who initiated a direct transfer trip to a registered entity's transmission breaker.

In situations where a Misoperation cause emanates from a non-registered outside entity, there may be limited influence an entity can exert on an outside entity and is considered outside of an entity's control.

The following in an example of a declaration made why corrective actions would not improve BES reliability.

**Example R5g:** The investigation showed that the Misoperation occurred due to transients associated with energizing transformer ABC at Station Y. Studies show that de-sensitizing the relay to the recorded transients may cause the relay to fail to operate as intended during power system oscillations.

**Example R5h:** As a result of an operation that left a portion of the power system in an electrical island condition, circuit XYZ within that island tripped, resulting in loss of load within the island. Subsequent investigation showed an overfrequency condition persisted after the formation of that island and the XYZ line protective relay operated. Since this relay was operating outside of its designed frequency range and would not be subject to this condition when line XYZ is operated normally connected to the BES, no corrective action will be taken because BES reliability would not be improved.

**Example R5i:** During a major ice storm, four of six circuits were lost at Station A. Subsequent to the loss of these circuits, a skywire (i.e., shield wire) broke near station A on line AB (between Station A and B) resulting in a phase-phase fault. The protection scheme utilized for both protection groups is a POTT. The Line AB protection at Station B tripped timed for this event (i.e., Slow Trip – During Fault) even though this line had been identified as requiring high speed clearing. A weak infeed condition was created at Station A due to the loss of 4 transmission circuits resulting in the absence of a permissive signal on Line AB from Station A during this fault. No corrective action will be taken for this Misoperation as even under N-1 conditions, there is normally enough infeed at Station A to send a proper permissive signal to station B. Any changes to the protection scheme to account for this would not improve BES reliability.

A declaration why corrective actions are beyond the entity's control or would not improve BES reliability should include the Misoperation cause and the justification for taking no corrective action. Furthermore, a declaration that no further corrective actions will be taken is expected to be used sparingly.

## Requirement R6

To achieve the stated purpose of this standard, which is to identify and correct the causes of Misoperations of Protection Systems for BES Elements, the responsible entity is required to implement a CAP that addresses the specific problem (i.e., cause(s) of the Misoperation) through completion. Protection System owners are required in the implementation of a CAP to update it when actions or timetable change, until completed. Accomplishing this objective is intended to reduce the occurrence of future Misoperations of a similar nature, thereby improving reliability and minimizing risk to the BES.

The following is an example of a completed CAP for a relay Misoperation that was applying a standing trip (See also, Example R5a).

**Example R6a:** Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. The failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.

CAP completed on 06/25/2014.

The following is an example of a completed CAP for a relay Misoperation that was applying a standing trip that resulted in the correction and the establishment of a program for further replacements (See also, Example R5b).

**Example R6b:** Actions: The impedance relay was removed from service on 06/02/2014 because it was applying a standing trip. The failed capacitor was found within the impedance relay and replaced. The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on 06/05/2014.

A program for wholesale preemptive replacement of capacitors in this type of impedance relay was established on 10/28/~~12~~2014.

CAP ~~Example 3 - Corrective~~completed on 10/28/2014.

The following is an example of a completed CAP of corrective actions with a timetable that required updating for a failed relay; and preemptive actions for similar installations~~:~~ (See also, Example R5c).

**Example R6c:** Actions: The impedance relay was removed from service on ~~6/2/12~~06/02/2014 because it was applying a standing trip. ~~Relay testing was performed on 6/4/12. A~~The failed capacitor was found within the impedance relay~~. The capacitor was~~ and replaced ~~on 6/5/12. .~~ The impedance relay functioned properly during testing after the capacitor was replaced. The impedance relay was returned to service on ~~6/5/12~~06/05/2014.

~~Applicability to other Protection Systems: Undesired trips of this type of~~The impedance relay ~~due to~~ capacitor ~~failures have occurred frequently. It is therefore our assessment that preemptive~~ replacement ~~of capacitors in this type of impedance relay should be pursued.~~

~~It is planned to replace the impedance relay capacitors~~was completed at stations A, B, and C ~~by 9/1/12. It is planned to replace the~~on 08/16/2014. The impedance relay ~~capacitors~~capacitor replacement was completed at stations D, E, and F ~~by 11/1/12. It is planned to replace the~~on 10/24/2014. The impedance relay ~~capacitors at~~capacitor replacement for stations G, H, and I ~~by 2/1/13.~~

~~The impedance relay~~were postponed due resource rescheduling from 02/01/15 to 03/01/2015. Following the timetable change, capacitor replacement was completed ~~at stations A, B, and C on 8/16/12. The impedance relay capacitor replacement was completed at stations D, E, and F on 10/26/12. The impedance relay capacitor replacement was completed at stations~~ on 03/09/2015 at stations G, H, and I ~~on 1/9/13~~. All stations identified in the evaluation have been completed.

CAP ~~Example 4 - Corrective~~completed on 03/09/2015.

The following is an example of a completed CAP for corrective actions with updated actions for a firmware problem; and preemptive actions for similar installations~~:~~. (See also, Example R5d).

**Example R6d:** Actions: Fault records were provided to the manufacturer on ~~6/4/12. On 6/11/12, the~~06/04/2014. The manufacturer responded that the ~~m~~Misoperation was caused by a bug in version 2 firmware, and recommended installing version 3 firmware. Version 3 firmware was installed on ~~6~~08/12/~~12~~2014.

~~Applicability~~Nine of the twelve relays were updated to ~~other Protection Systems: Based on our risk assessment, we plan to install firmware~~ version 3 ~~at all of our installations that are~~ firmware on 09/23/2014. The manufacturer provided a subsequent update which was

determined to be beneficial for the remaining relays. The remaining three of twelve relays identified as having the version 2. Proposed completion date is 12/31/12.

The firmware replacements were were updated to version 3.01 firmware on 11/10/2014.

CAP completed on 12/4/1211/10/2014.

IfThe CAP is complete when all the documented actions to resolve the specific problem (i.e., Misoperation cause is identified within 120 days, and no corrective action has been or is intended to be taken, Protection System owners) are required to make a declaration to this effect. A "no CAP declaration" would typically completed which may include the Misoperation cause and justification for taking no corrective action.

An examplethose actions resulting from the entity's evaluation of other locations, if not addressed through a separate CAP.

**Process Flow Chart:** Below is a ~~"no CAP declaration" due to BES reliability might be: "The investigation showed the Misoperation occurred due to transients associated with energizing transformer ABC at Station Y. Our studies show that de-sensitizing~~ graphical representation of the ~~relay to the recorded transients may cause the relay to fail to operate as intended during power system oscillations." A "no CAP declaration" due to BES reliability is~~ expected ~~to be used sparingly.~~

~~There are some cases where a Misoperation cause is outside of an entity's control and would result in a "no CAP declaration." Items that may be considered outside of an entity's control could be a non-registered entity communications provider problem or a transmission transformer tapped industrial customer who initiates a direct transfer trip to a registered entity's transmission breaker. Generally, situations where a Misoperation cause emanates from a non-registered outside entity, there may be limited influence an entity can exert on an outside entity and is considered outside of an entity's control. The "outside an entity's control" declaration is expected to be used sparingly.~~

**~~Requirement R3~~**

~~If the Misoperation cause is not identified within 120 days, and reasonable investigative actions have not been exhausted, Protection System owners are expected to exercise due diligence in the development and implementation of an action plan for additional investigation. This action plan would typically include any investigative actions taken to determine the cause (along with the date performed), and any investigative actions planned to be taken to determine the cause (along with the planned date).~~

~~At the end of 180 days, the Protection System owner must have an action plan or a declaration why no further actions will be taken. The action plan does not need to have been implemented within the 180 days, but it must have been developed within this time frame. The 180 calendar days are the sum of 120 calendar days (investigative period in Requirement R1) and a 60 calendar day period (similar timeframe as in Requirement R2 for developing a CAP.)~~

~~Where there are multiple Protection System owners involved in a Misoperation and no cause has been determined, then each Protection System owner must either develop an action plan or declare why no further actions will be taken.~~

~~An example of an investigative action plan for more testing might be: "All relays at station A functioned properly during testing on xx/xx/xx. An outage is required to test the relays at station B. The outage is scheduled for xx/xx/xx."~~

~~An example of an action plan for adding monitoring might be: "All relays at station A and B functioned properly during testing on xx/xx/xx. It is planned to install a temporary DFR at station A on xx/xx/xx and to monitor the currents for at least 3 months."~~

~~An example of an action plan for reviewing relay settings might be: "All relays at station A functioned properly during testing on xx/xx/xx. All relays at station B functioned properly during testing on xx/xx/xx. The carrier system functioned properly during testing on xx/xx/xx. It is planned to complete a relay settings review~~ process created by ~~xx/xx/xx."~~

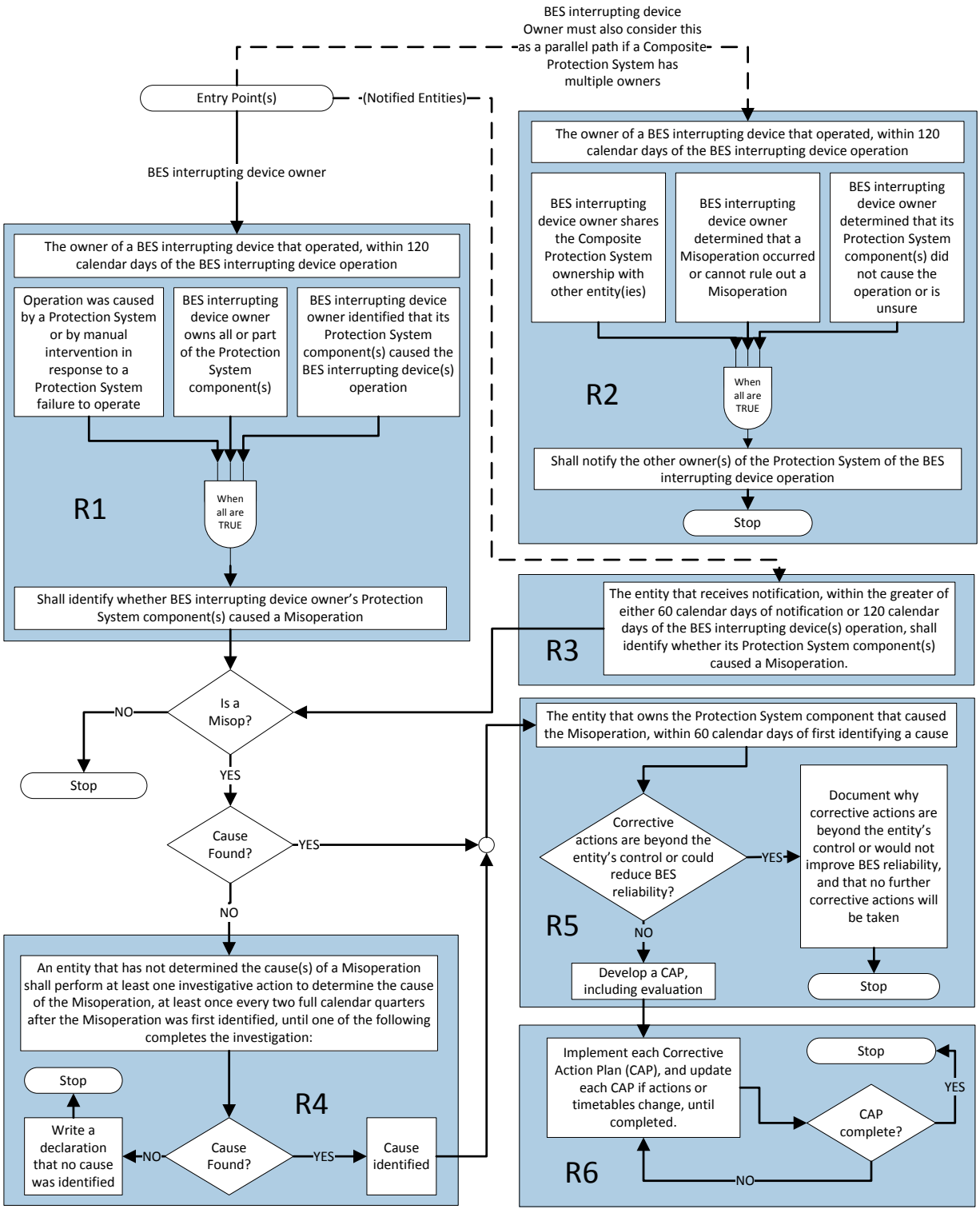
~~If the Misoperation cause is not identified and reasonable investigative actions have been exhausted within 180 days, Protection System owners are required to make a declaration to this~~

effect. A "no action plan" declaration would typically include any investigative actions taken to determine the cause (along with the date performed), and justification for taking no additional investigative actions.

An example of a "no action plan" declaration might be: "All relays at station A and B functioned properly during testing on xx/xx/xx. The carrier system functioned properly during testing on xx/xx/xx. The carrier coupling equipment functioned properly during testing on xx/xx/xx. A settings review completed on xx/xx/xx indicated the relay settings were proper. Since the equipment involved in the operation functioned properly during testing, the settings were reviewed and found to be proper, and the equipment at station A and station B is already monitored, we have decided to close this investigation."

**Requirement R4**

The goal of the standard has not been met unless CAPs or action plans are actually implemented, as is required in Requirement R4. The responsible entity is required to implement and complete a CAP or action plan to accomplish the purpose of this standard, which is to prevent future Misoperations, thereby minimizing risk to the BES. The responsible entity is also required to complete the CAP or action plan, document the plan implementation, and retain the appropriate evidence to demonstrate implementation and completion., including the relationships between requirements:




~~The goal of an action plan created in Requirement R3 is to determine a cause so a CAP can be created to ultimately remedy the cause of the Misoperation. If the cause is determined as a result of the action plan, the entity must develop a CAP or a declaration within 60 days of determination of cause per Requirement R2. This requirement sets the expectation that the work identified in the CAP or action plan will be completed on schedule as planned. Deferrals or~~

~~other relevant changes to the CAP or action plan need to be documented so that the record includes not only what was planned, but what was implemented. Depending on the planning and documentation format used by the responsible entity, evidence of successful CAP or action plan execution could consist of signed-off work orders, printouts from work management systems, spreadsheets of planned versus completed work, timesheets, work inspection reports, paid invoices, photographs, walk-through reports or other evidence.~~

~~Documentation of a CAP or action plan provides an auditable progress and completion confirmation for specific Misoperations. In addition, the investigative documentation may aid the responsible entity in remedying future Misoperations of a similar nature.~~